Il Sole 24 ORE

Data 16-05-2023
Pagina 38
Foglio 1 / 2

Sui rischi informatici in prima linea gli operatori finanziari

Dora

Il regolamento Ue vincolerà le imprese dal 17 gennaio 2025

Giuseila Finocchiaro
Oreste Pollicino
Flavia Scarpellini

Dopo il clamore di Chatgpt e la conferma dell'imminente regolamentazione Ue dell'intelligenza artificiale, recenti interventi normativi hanno definitivamente suggellato, se ce ne fosse stato bisogno, la centralità della tecnologia digitale e la necessità, da una parte, di non alzare una saracinesca nei confronti dell'innovazione e, dall'altra parte, di un attento esercizio di valutazione e ponderazione dei possibili rischi.

Basti pensare, a titolo esemplificativo, innanzitutto, al nuovo codice degli appalti dettato dal Dlgs 36/2023, che prevede in modo massivo la digitalizzazione delle gare e l'uso dell'intelligenza artificiale (e delle tecnologie dei registri distribuiti) anche per le analisi delle offerte, per passare alla digitalizzazione degli strumenti finanziari (Dl 25 del 17 marzo 2023) anche per le Spa e le Srl.

In pratica, le imprese non potranno più operare senza fare i conti con investimenti digitali di un certo rilievo, pena l'esclusione da taluni mercati e la crescente difficoltà ad operare quotidianamente, anche per tenere una semplice assemblea di una Srl "tokenizzata".

L'adozione della tecnologia porta con sé i relativi rischi, come le recenti cronache (si veda da ultimo il recente attacco hacker all'Asl 1 Abruzzo) testimoniano: rischio economico (blocco delle attività, perdita dei dati), gestionale, sanzionatorio (violazione della privacy) e reputazionale.

Si tratta di rischi che possono e devono essere affrontati nell'interesse dell'azienda e della sicurezza della rete interconnessa dell'intero Paese.

A questo proposito, il Regolamento Ue cosiddetto "Dora" (*Digital operational resilience act*) 2022/2554 del 14 dicembre 2022 - entrato in vigore il 18 gennaio scorso con un grace period di 24 mesi - ha introdotto specifici obblighi in materia di rischi informatici direttamente in capo ai consigli di amministrazione di una vasta platea di operatori finanziari (oltre agli enti creditizi, istituti di pagamento e di moneta elettronica, imprese di investimento, fornitori di servizi per le cripto-attività autorizzati ed emittenti di token, depositari centrali di titoli, sedi di negoziazione, gestori di fondi di investimento alternativi, società di gestione, imprese di assicurazione e di riassicurazione, intermediari assicurativi e riassicurativi, enti pensionistici, agenzie di rating del credito, fornitori di servizi di crowdfunding, repertori di dati sulle cartolarizzazioni e relativi fornitori terzi di servizi Itc).

Tali incombenti possono costituire, per rilevanza e tempistica, un utile benchmark in tema di resilienza operativa digitale anche per le società non finanziarie (si veda «L'evoluzione dell'organo amministrativo tra sostenibilità e trasformazione digitale», gruppo di lavoro giunta Assonime coordinato da Corrado Passera, 2023).

Del resto, accade spesso che la normativa in ambito finanziario abbia anticipato e stabilito best practice per gli altri settori.

In base al regolamento, l'organo amministrativo è chiamato a definire, approvare l'attuazione e vigilare su uno «specifico quadro di gestione e controllo interno» di tutti i rischi informatici (Ict o Cit), definendo l'organigramma delle funzioni rilevanti, i flussi informativi, il relativo budget e istituendo una «funzione di garanzia dei rischi informatici» indipendente oltre all'internal audit.

Non è tutto. Dora richiede il presidio anche dei rischi operativi legati all'affidamento a terzi dei servizi Ict, evidenziando che l'outsourcing non elimina la relativa responsabilità da parte dell'azienda che esternalizza (che amplia il proprio perimetro) e potrebbe creare rischi di concentrazione.

Così, i fornitori devono essere oggetto di due diligence preventiva, con specifica valutazione dei conflitti di interessi, il contratto deve contenere minime clausole standard (in corso di emanazione) - comprensive di service level agreement (Sla), clausole di exit e di compliance - e divenire oggetto di specifici flussi informativi verso il Consiglio di amministrazione, con presidio esercitato da una figura interna chiamata a svolgere il monitoraggio del contratto.

L'approccio, quindi, si articola su un duplice livello:

- di governance/organizzativo (adozione di una sorta di modello organizzativo, con flussi informativi specifici sulla falsariga del modello 231 in tema di responsabilità delle imprese e dei presidi di cui al Gdpr in materia di privacy)
- e un livello contrattuale (*make or buy*, accurata scelta del fornitore e disciplina negoziale).

Senza dimenticare il necessario raccordo con la normativa sulla privacy (Gdpr) che costituisce il necessario complemento alla cybersecurity.

Naturalmente l'adozione di questi strumenti va calibrata, come previsto dal Regolamento Dora, in base alle dimensioni dell'impresa, ma è chiara la chiamata in responsabilità di imprenditori e organi amministrativi che non potranno più delegare, come in passato, la problematica del rischio digitale al management.

Il digital è un asset con cui le imprese si interfacciano regolarmente con il mondo e assumono decisioni, elaborando i dati che hanno a disposizione.

La disintermediazione, la progressiva trasformazione dei prodotti in servizi e la crescente affermazione di un marketplace virtuale (come il metaverso) inducono a ritenere non più differibile la presenza parallela anche di un'offerta digitale di prodotti e servizi in tutti i settori, compresi quelli più tradizionali.

I PRESÌDI
Responsabili imprenditori e organi amministrativi tenendo conto della dimensione d'impresa

LO STRUMENTO
Il contratto deve contenere clausole minime standard. Accurata scelta del fornitore


Riparte la riforma della bancarotta da riconciliare al Codice della crisi

TASSAZIONE DEGLI IMMOBILI